View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Tamkang University Institutional Repository

Security Weaknesses of Song's Advanced Smart Card Based Password Authentication Protocol

Wen-Bing Horng, Cheng-Ping Lee
Dept. Computer Science & Information Engineering
Tamkang University
Taipei, Taiwan, R.O.C.
E-mail: horng@mail.tku.edu.tw
Selrahc.charles@msa.hinet.net

Jian-Wen Peng
Dept. Commerce Technology & Management
Chihlee Institute of Technology
Taipei, Taiwan, R.O.C.
E-mail: pchw8598@mail.chilee.edu.tw

Abstract—**Password based authentication with smart cards has been adopted as a more secure means in insecure networks to validate the legitimacy of users. Traditional authentication schemes are based on the tamper-resistant smart card; that is, the data stored in the smart card cannot be revealed. However, it is a challenging problem for considering non-tamper-resistant smart cards used in user authentication. Very recently, in 2010, Song proposed an efficient authentication scheme with such non-tamper resistant smart cards based on symmetric key crypto-systems as well as modular exponentiations. In this paper, we will show that Song's scheme is vulnerable to the offline password guessing attack and the insider attack. Besides, this scheme does not provide perfect forward secrecy and does not preserve user anonymity.**

Keywords-network security; password based authentication; smart card

I. INTRODUCTION

Over insecure networks, it has been a common approach to authenticate users with passwords. In 1981, Lamport [1] proposed a one-time password remote authentication scheme using hash chains, and later, in 1994, Haller [2] presented a practical S/KEY one-time password system. However, these two schemes need to maintain a verification table in the remote server to verify user's legitimacy. Thus, such methods are vulnerable to the stolen-verifier attack and the modification attack on the verification table.

The smart card is an emerging technology. It consists of a microprocessor and memory (RAM and ROM) so that it can perform arithmetic/logic operations and store some user information. Thus, it has been widely applied to enhance remote user authentication, as in [3–18]. In a typical smart card based password authentication scheme, a remote server only needs to maintain a common secret key, instead of storing a verification table to avoid the above drawbacks.

The evolution of smart card based authentication schemes consists of the following security features:

- no verification table required,
- letting users choose their own passwords,
- supporting mutual authentication,
- providing session keys for secure communications,
- providing perfect forward secrecy for session keys even if users' passwords are compromised,
- protecting user anonymity to preserve user privacy,
- should be efficient and practical, and
- withstanding various kinds of attacks, such as replay attack, offline password guessing attack, user impersonation attack, server spoofing attack, man-in-the-middle attack, and so on.

Note that the above security features provided by the authentication schemes [3–10] are based on the assumption that the smart card is tamper-resistant. However, Kocher et al. [19] and Messerges et al. [20] pointed out that the stored information in the smart card can be obtained through monitoring the power consumption or by analyzing the leaked information. Therefore, the smart card is no longer a tamper-resistant device, and, thus, those schemes based on the tamper-resistant assumption become insecure if the smart card is compromised. For example, as reported in [17], Lee-Chiu's scheme [7] is vulnerable to the user impersonation attack and Lee-Kim-Yoo's scheme [8] is subject to the offline password guessing attack if the data stored in the smart card can be revealed.

Therefore, it is a challenge to design a more secure password based authentication with non-tamper-resistant smart cards. To cope with the information leakage problem with such non-tamper-resistant smart cards, several advanced authentication schemes [11–18] have been proposed. Recently, Xu et al. [17] presented a password authentication scheme using such non-tamper-resistant smart cards based on costly modular exponentiations. However, Song [18] demonstrated that Xu et al.'s scheme is vulnerable to the user impersonation attack and proposed a new and more efficient authentication scheme based on symmetric-key cryptosystems and modular exponentiations.

In this paper, we will show that Songs scheme is vulnerable to the offline password guessing attack and the insider attack. In addition, this scheme does not provide perfect forward secrecy for session keys. Besides, it does not protect user anonymity to preserve user privacy.

The rest of the paper is organized as follows. In Section 2, we briefly review Songs smart card based password

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC 98-2631-S-032-003.

978-1-4244-6789-1/10/$26.00 ©2010 IEEE

authentication protocol. In Section 3, we demonstrate the security weaknesses of Songs scheme. We conclude this paper in the last section.

II. Review of Song's Authentication Protocol

In this section, we briefly review Songs scheme [18], as depicted in Fig. 1. This scheme is based on a hybrid approach using both symmetric key cryptosystems and modular exponentiations. It consists of five phases: initial phase, registration phase, login phase, authentication phase, and password change phase. The notation used in this paper is listed below.

- U : a user (client)
- ID : the identity of U
- PW : the password of U
- S : a remote server
- X : the secret key of S
- $h(\cdot)$: a secure one-way hash function
- $E_K(M)$: symmetric encryption of message M with secret key K
- $D_K(M)$: symmetric decryption of message M with secret key K
- $\oplus$: the bitwise XOR operation
- $||$: the concatenation operation

A. Initial Phase

The remote server S first chooses a secret key x and two large primes p and q such that $p = 2q + 1$. Then, S selects a secure one-way hash function $h(\cdot)$ and a symmetric key cryptography algorithm with encryption $E(\cdot)$ and decryption $D(\cdot)$ operations, such as DES and AES. The server S keeps x, p, and q secret.

B. Registration Phase

A user U submits his/her ID and PW to a remote server S through a secure channel for registration. If S accepts U's registration request, it computes $B = h(ID^x \bmod p) \oplus h(PW)$. Then, S issues U a smart card containing $\{ID, B, h(\cdot), E(\cdot)\}$ over a secure channel.

C. Login Phase

If U wants to login to S, he/she inserts his/her smart card into a card reader and inputs his/her ID and PW. The smart card first generates a random number R. Then, it computes $K = B \oplus h(PW)$, $W = E_K(R \oplus T_U)$, and $C_U = h(T_U \,||\, R \,||\, W \,||\, ID)$, where T_U is the current timestamp. Finally, the smart card sends the login request message $\{ID, C_U, W, T_U\}$ to S.

D. Authentication Phase

1) *User Authentication*: Upon receiving the login request from user U at time T', the server S first validates the user's identity ID and checks whether $(T' - T_U) \le \Delta T$, where ΔT is a predefined transmission delay. If either one fails, the login request is rejected. The server S then computes $K = h(ID^x \bmod p)$ and $R' = D_K(W) \oplus T_U$, and checks whether $h(T_U \,||\, R' \,||\, W \,||\, ID) = C_U$. If they are equal, the user U is authenticated, and the sever S accepts the login request; otherwise, reject the request. Finally, S computes $C_S = h(ID \,||\, R' \,||\, T_S)$ and sends the reply message $\{ID, C_S, T_S\}$ to U, where T_S is the current timestamp.

2) *Server Authentication*: After receiving the reply message from S, the smart card first validates ID and checks the freshness of T_S. Then, it checks whether $h(ID \,||\, R \,||\, T_S) = C_S$. If they are equal, the server is authenticated; otherwise, stop the connection.

3) *Session Key Establishment*: After successful mutual authentication, both U and S compute the shared session key $sk = h(ID \,||\, T_S \,||\, T_U \,||\, R)$ for subsequent secure communications.

E. Password Change Phase

If the user U wants to change his/her password, he/she inserts his/her smart card into a card reader and inputs his/her ID and PW. Then, a mutual authentication between the server S and the smart card is performed first. Once the authentication is complete, the smart card first asks U to enter a new password PW'. Then, it computes $B' = B \oplus h(PW) \oplus h(PW')$ and replaces B with B' to complete the password change phase.

III. Weakness of Song's Protocol

In this section, we will show that Song's scheme [18] is vulnerable to the offline password guessing attack and the insider attack. In addition, the scheme does not provide perfect forward secrecy for session keys. Besides, it does not preserve user anonymity and, thus, is subject to tracking.

A. Offline Password Guessing Attack

A remote user authentication scheme vulnerable to the offline password guessing attack must satisfy the two conditions: the user's password is weak, and there exists a piece of password-related information used as a comparison target for password guessing. In Song's scheme, a user U is allowed to choose his/her own password at will during the registration phase. In general, the user tends to select a password that is easily to remember for his/her convenience. Hence, such easy-to-remember passwords (also called *weak passwords*) are potentially vulnerable to the offline password guessing attack, in which an adversary may try to guess the user's password from a dictionary of all possible weak passwords and then verify the guess.

On the other hand, Song's scheme assumes that the smart card is non-tamper-resistant (i.e., the information stored in the smart card can be revealed). If an adversary has retrieved B stored in U's smart card and has intercepted the messages transmitted between U and S in one of previous sessions, such as $\{ID, C_U, W, T_U\}$ and $\{ID, C_S, T_S\}$, then the adversary can mount an offline password guessing attack as follows. He first guesses a new password PW^* and computes $K^* = B \oplus h(PW^*)$. Then, the adversary calculates $R^* = D_{K^*}(W) \oplus T_U$ and checks whether $h(T_U \,||\, R^* \,||\, W \,||\, ID) = C_U$ (or $h(ID \,||\, R^* \,||\, T_S) = C_S$). If they are equal, the guessed password PW^* is correct; otherwise, continues another guess until the correct password is found or run out of the weak password dictionary.

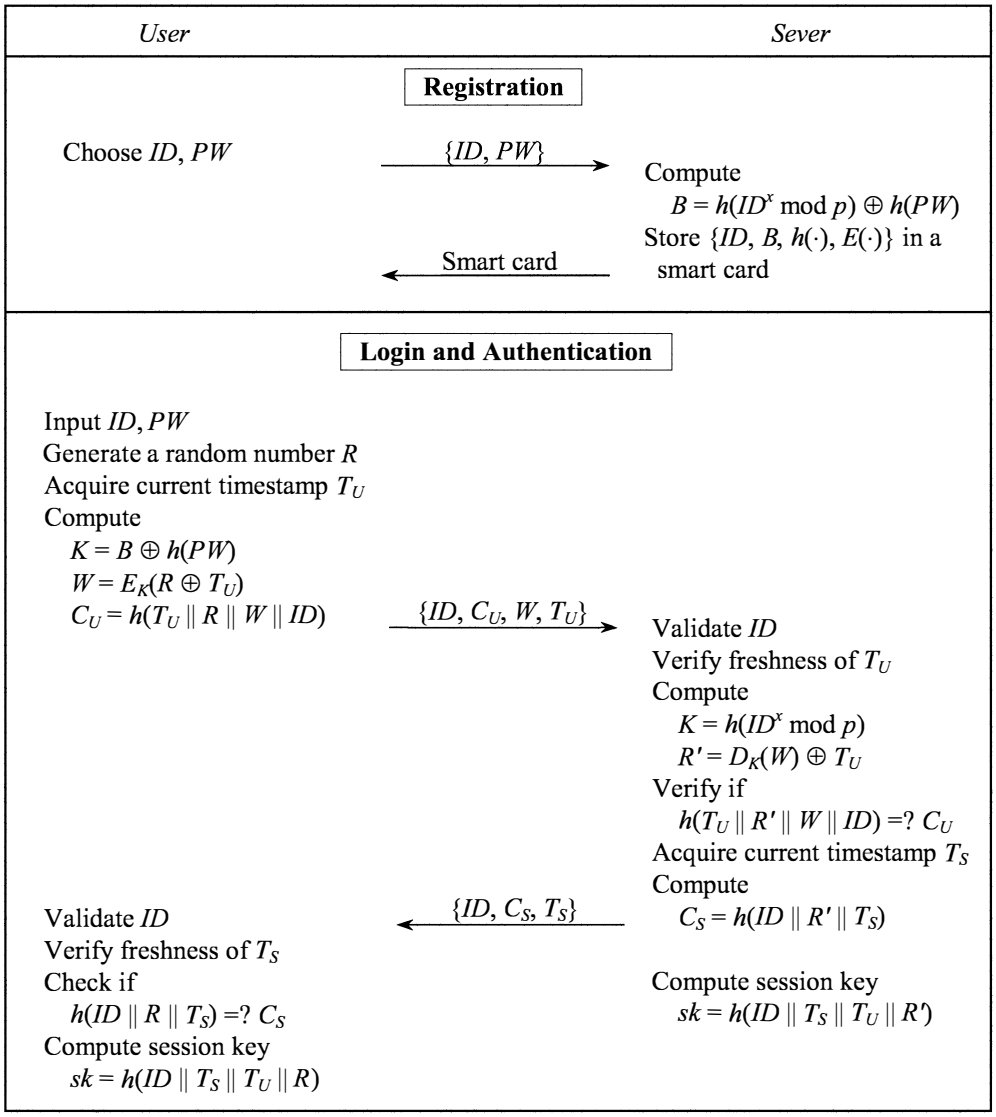

Figure 1. Song's authentication protocol

B. *Insider Attack*

It is a common practice in the real world that many users use the same passwords to access different servers for their convenience without remembering different passwords for different servers. However, if a privileged insider (such as the system manager) of the server S knows the password of a user U, he may try to impersonate U by accessing other servers where U has registered. In Song's scheme, U sends his/her ID and PW in plaintext form to S during the registration phase. Thus, this scheme may suffer from the insider attack [5] if a privileged insider comes to know the password PW of a registered user U and misuses it.

C. *Lack of Perfect Forward Secrecy*

Perfect forward secrecy is an important security property for session key distribution; it means that if a long-term secret (e.g., a user's password in a password based authentication protocol) is compromised, the session keys of past sessions still cannot be derived. In Song's scheme, once U's password PW is compromised, session keys used in previous sessions will be computed as follows. Suppose that an adversary has retrieved B stored in U's smart card and has intercepted messages $\{ID, C_U, W, T_U\}$ and $\{ID, C_S, T_S\}$ transmitted in a previous session, then the adversary can derive the session key used in that session by computing $K = B \oplus h(PW)$ and $R = D_K(W) \oplus T_U$. Finally, the adversary can obtain the session key by computing $sk = h(ID \| T_S \| T_U \| R)$.

D. *Not preserving user anonymity*

Recently, preserving user anonymity has become an important issue since it can prevent users from tracking. However, in Song's scheme, it does not preserve user anonymity because the user's identity ID is transmitted over the network in plaintext form. Hence, in this scheme, the user anonymity is not preserved and is vulnerable to tracking.

IV. CONCLUSION

In this paper, we have demonstrated that Song's smart card based password authentication scheme is vulnerable to the offline password guessing attack and the insider attack. Besides, it cannot protect user anonymity to preserve user privacy such that users can be tracked. In addition, it does not provide perfect forward secrecy for session keys such that all previous communications can be decrypted with session keys if passwords are compromised.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable comments and constructive suggestions.

REFERENCES

[1] L. Lamport, "Password authentication with insecure communication," Commun. ACM, vol. 24, no. 11, pp. 770–772, 1981.

[2] N. M. Haller, "The S/KEY one-time password system," Proc. ISOC Symposium on Network and Distributed System Security, San Diego, CA, 1994, pp. 151–157.

[3] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "An efficient and practical solution to remote authentication: smart card," Comput. Secur., vol. 21, no. 4, pp. 372–375, 2002.

[4] M. S. Hwang, C. C. Lee, and Y. L. Tang, "A simple remote user authentication scheme," Math. Comput. Model., vol. 36, no. 1–2, pp. 103-107, 2002.

[5] W. C. Ku and S. M. Chen, "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards," IEEE Trans. Consum. Electron., vol. 50, no. 1, pp. 204–207, 2004.

[6] W. S. Juang, "Efficient password authenticated key agreement using smart cards," Comput. Secur., vol. 23, no. 2, 167–173, 2004.

[7] N. Y. Lee and Y. C. Chiu, "Improved remote authentication scheme with smart card," Comput. Stand. Interfaces, vol. 27, no. 2, pp. 177–180, 2005.

[8] S. W. Lee, H. S. Kim, and K. Y. Yoo, "Improvement of Chien et al.'s remote user authentication scheme using smart cards," Comput. Stand. Interfaces, vol. 27, no. 2, pp. 181–183, 2005.

[9] H. T. Liaw, J. F. Lin, and W. C. Wu, "An efficient and complete remote user authentication scheme using smart cards," Math. Comput. Model., vol. 44, no. 1–2, pp. 223–228, 2006.

[10] W. G. Shieh and J. M. Wang, "Efficient remote mutual authentication and key agreement," Comput. Secur., vol. 25, no. 1, pp. 72–77, 2006.

[11] C. I. Fan, Y. C. Chan, and Z. K. Zhang, "Robust remote authentication scheme with smart cards," Comput. Secur., vol. 24, no. 8, pp. 619–628, 2005.

[12] I. E. Liao, C. C. Lee, and M. S. Hwang, "A password authentication scheme over insecure networks," J. Comput. Syst. Sci., vol. 72, no. 4, pp. 727–740, 2006.

[13] X. M. Wang, W. F. Zhang, J. S. Zhang, M. K. Khan, "Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards," Comput. Stand. Interfaces, vol. 29, no. 5, pp. 507–512, 2007.

[14] W. S. Juang, S. T. Chen, and H. T. Liaw, "Robust and efficient password-authenticated key agreement using smart cards, IEEE Trans. Ind. Electron., vol. 55, no. 6, pp. 2551–2556, 2008.

[15] W. S. Juang and W. K. Nien, "Efficient password authenticated key agreement using bilinear pairings," Math. Comput. Model., vol. 47, no. 11–12, pp. 1238-1245, 2008.

[16] H. R. Chung, W. C. Ku, M. J. Tsaur, "Weaknesses and improvement of Wang et al.'s remote user password authentication scheme for resource-limited environments," Comput. Stand. Interfaces, vol. 31, no. 4, pp. 863–868, 2009.

[17] J. Xu, W. T. Zhu, D. G. Feng, "An improved smart card based password authentication scheme with provable security," Comput. Stand. Interfaces, vol. 31, no. 4, pp. 723–728, 2009.

[18] R. Song, "Advanced smart card based password authentication protocol," Comput. Stand. Interfaces, vol. 32, no. 5–6, pp. 321–325, 2010.

[19] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," Proc. Advances in Cryptology (LNCS 1666), 1999, pp. 388–397.

[20] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," IEEE Trans. Comput., vol. 51, no. 5, pp. 541–552, 2002.